Kódoláselmélet 2020 november 18.

Feladat: Határozzuk meg az összes bináris 7-hosszúságú ciklikus lineáris kódot.

$$K = \mathbb{Z}_2$$

Meg kell határozni az x^7-1 -nek a valódi osztóit.
$x^7-1 = x^7+1$ $\mathbb{Z}_2[x]$-ben

$$x^7+1 = (x+1)(\underbrace{x^6+x^5+x^4+x^3+x^2+x+1}_{\text{nincs gyöke}})$$

ha ez nem irred, akkor 2 és 4-edfokú szorzatára vagy 3+3 fokú szorzatára bontható.

2-odfokú irred x^2+x+1 van csak
3-adfokú x^3+x+1 és x^3+x^2+1.

$$x^6+x^5+x^4+x^3+x^2+x+1 \div x^3+x+1 = x^3+x^2+1$$
$$\frac{-(x^6+x^4+x^3)}{x^5+x^2+x+1}$$
$$\frac{-(x^5+x^3+x^2)}{x^3+x+1}$$

$$x^7+1 = (x+1)(x^3+x+1)(x^3+x^2+1) \quad \text{irred felbontás.}$$

valódi osztók 7 db

$g_1 = 1$
$g_2 = x+1$
$g_3 = x^3+x+1$
$g_4 = x^3+x^2+1 \longleftarrow G_4 = \begin{pmatrix} 1&0&1&1&0&0&0\\ 0&1&0&1&1&0&0\\ 0&0&1&0&1&1&0\\ 0&0&0&1&0&1&1 \end{pmatrix}$
$g_5 = (x+1)(x^3+x+1)$
$g_6 = (x+1)(x^3+x^2+1)$
$g_7 = (x^3+x+1)(x^3+x^2+1)$

Áll: Ez G_4 éppen egy Hamming-kód

$$\begin{pmatrix} 1&0&1&1&0&0&0 \\ 0&1&0&1&1&0&0 \\ 0&0&1&0&1&1&0 \\ 0&0&0&1&0&1&1 \end{pmatrix} \rightsquigarrow \left(\begin{array}{cccc|ccc} 1&0&0&0&1&0&1 \\ 0&1&0&0&1&1&1 \\ 0&0&1&0&1&1&0 \\ 0&0&0&1&0&1&1 \end{array}\right)$$

$(E \ H)$

ellenőrző mátrix $P = \begin{pmatrix} -H \\ E \end{pmatrix} = \left(\begin{array}{ccc} 1&0&1 \\ 1&1&1 \\ 1&1&0 \\ 0&1&1 \\ \hline 1&0&0 \\ 0&1&0 \\ 0&0&1 \end{array}\right)$

ez egy Hamming kód.

Def: K tetszőleges test, $f \in K[x]$ r-edfokú irreducibilis polinom, $0 \neq \alpha \in K[x]/\langle f \rangle$ egy legalább n-edrendű eleme, $d \leq n$ és $g \in K[x]$ az $\alpha, \alpha^2, \ldots, \alpha^{d-1}$ elemek minimálpolinomjainak legkisebb közös többszöröse. Ekkor g által generált n-hosszú lineáris kódot BCH-kódnak nevezzük a d tervezett távolsággal.

Bose, Ray-Chaudhuri, Hocquenghem feltalálók.

Tétel: A fenti paraméterekkel

① a kód hossza $n \leq |K|^r - 1$ ← ez a max elemrend ami lehet.

② minimális távolsága legalább d.

③ dimenziója $n - \deg(g) \geq n - r(d-1)$

④ ciklikus ha $n = o(\alpha)$.

Előismeretek

Tétel: K test, $f \in K[x]$ irred $\Rightarrow$ $K[x]/\langle f\rangle$ ez test.

Biz: $K[x]$ egységelemes kommutatív gyűrű, tehát

$K[x]/\langle f\rangle = \{\underbrace{g + \langle f\rangle}\ |\ g \in K[x]\}$

$\langle f\rangle = \{hf\ |\ h \in K[x]\}$ főideál

mellékosztályai

faktorgyűrű is egységelemes és kommutatív.

Az egyetlen érdekes kérdés, hogy minden nem 0 elemnek van-e ~~inverze~~ inverze.

$\bar g = g + \langle f\rangle \in K[x]/\langle f\rangle$ $\qquad \bar g \neq \bar 0$

$gu + fv = 1$ diofantoszi egyenlet

megoldható-e $K[x]$-ben u-ra és v-re?

$\mathrm{lnko}(g,f) \mid 1$ de ez teljesül, mert

f osztói f asszociáltjai és 1 asszociáltjai.

$\mathrm{lnko}(g,f) \sim 1$ vagy $\mathrm{lnko}(g,f) \sim f$

ez nem lehet, mert

$f \mid g \Leftrightarrow \bar g = \bar 0$

ez teljesül, azaz a diofantoszi egyenletnek van megoldása

$\bar f = \bar 0$

$\bar g \cdot \bar u + \bar f \cdot \bar v = \bar 1$

$\Downarrow$ meg van az inverz.

$\bar g \cdot \bar u = \bar 1$

Megj: Ez tetszőleges euklideszi gyűrűben így van, pl $\mathbb{Z}_p$

f ired polinom

Def: $\alpha \in K[x]/\langle f\rangle$ minimálpolinomja az a legkisebb fokszámú $g \in K[x]$ főpolinom, hogy $g(\alpha)=0$ teljesül a $K[x]/\langle f\rangle$ testben.

Áll: Minden elemnek van minimálpolinomja

(0)

(1) ami egyértelműen meghatározott

(2) $h \in K[x]$-re $h(\alpha)=0 \iff g \mid h$

(3) g irreducibilis

(5) $\deg(g) \leq r$

(4) $g \mid x^{|K|^r-1}-1$

Biz: (1) Ha $g_1(\alpha)=0$ $g_2(\alpha)=0$ ~~$g_1 \neq g_2$~~

$$\deg(g_1)=\deg(g_2)$$

$$(g_1-g_2)(\alpha)=g_1(\alpha)-g_2(\alpha)=0$$

$\deg(g_1-g_2) < \deg(g_1)$ mert a főegyüttható kiesik.

Ha $g_1 \neq g_2$, akkor a nem 0 g_1-g_2 polinomot egy alkalmas $c \in K$ skalárral megszorozva egy kisebb fokszámú $c(g_1-g_2)$ polinomot kapnuk, amelynek α gyöke.

(2) $h=gp \Rightarrow h(\alpha)=g(\alpha)\cdot p(\alpha)=0\cdot p(\alpha)=0$

$h=gq+r$ maradékos osztás $\deg(r)<\deg(g)$

$h(\alpha)=g(\alpha)q(\alpha)+r(\alpha)=r(\alpha)$

Ha $h(\alpha)=0 \Rightarrow r(\alpha)=0$ és a min fokszám miatt $r=0$ polinom lehet csak $\Rightarrow h=gq$.

3 Ha g nem irred, akkor

$$g = g_1 g_2 \qquad \underset{<}{\deg(g_1)} + \underset{<}{\deg(g_2)} = \deg(g)$$

$0 = g(\alpha) = g_1(\alpha) \cdot g_2(\alpha)$ ~~testben~~ $K[x]/\langle f \rangle$ testben.

ez csak úgy lehetséges,
hogy $g_1(\alpha)=0$ vagy $g_2(\alpha)=0$
De ez ellentmond g minimális fokszámának. ∎

<u>Példa</u>: $K = \mathbb{Z}_2 \quad f = x^3 + x + 1$

$$K[x]/\langle f \rangle = \{\bar{0}, \bar{1}, \bar{x}, \overline{x+1}, \overline{x^2}, \overline{x^2+1}, \overline{x^2+x}, \overline{x^2+x+1}\}$$

8-elemű test.

(Megj $\bar{x} \cdot \overline{x^2+1} = \overline{x^3+x} = \bar{1}$).

koordináta

$$\left.\begin{aligned} \alpha &= \bar{x} = (0,1,0) \\ \alpha^0 &= \bar{1} = (1,0,0) \\ \alpha^2 &= \overline{x^2} = (0,0,1) \\ \alpha^3 &= \overline{x+1} = (1,1,0) \end{aligned}\right\}$$

$K[x]/\langle f \rangle$ test vektortér K felett és egy bázisa $\bar{1}, \bar{x}, \overline{x^2}, \dots, \overline{x^{r-1}}$ ahol $r = \deg f$

4 vektor egy 3-dim vektortérben.
tehát $1, \alpha, \alpha^2, \alpha^3$ lin függő

$\overline{x^3} = \overline{x+1}$

$$1 \cdot \alpha^3 + 0 \cdot \alpha^2 + 1 \cdot \alpha + 1 \cdot \bar{1} = \bar{0}$$ nem triv lin komb.

$g = x^3 + x + 1 \qquad g(\alpha) = \alpha^3 + \alpha + \bar{1} = \bar{0}$, azaz
~~van~~ létezik minimál polinom

4 $g \mid x^{|K|^r-1}-1$ bizonyítása

$T = K[x]/\langle f \rangle$ test multiplikatív csoportja

$T^* = |K|^r-1$ elemű ciklikus csoport.

azaz minden elem rendje ~~a~~ $|K|^r-1$ osztója.

$o(\alpha) \mid |K|^r-1$

$\alpha^{|K|^r-1} = \bar{1}$

tehát α gyöke a $h = x^{|K|^r-1} - 1 \in K[x]$ polinomnak.

Biz (BCH kódok tétele)

2 α^1 min polinomja g_1

α^2 —//— g_2

$\vdots$

α^{d-1} g_{d-1}

$g = \text{lkkt}(g_1, g_2, \dots, g_{d-1}) \in K[x]$

$C = \{ gh \mid h \in K[x],\ \deg(h) < n - \deg(g) \}$

$\Downarrow$

$\deg(gh) < n$

generátor mátrix

$$G = \begin{pmatrix} g \\ gx \\ \vdots \\ gx^{n-\deg(g)-1} \end{pmatrix}$$

~~Kérdés, ho~~ Állítás, hogy $gh \in C$ $h \neq 0$ akkor gh-nak Hamming-távolsága a 0 vektortól legalább d.

7

Tfh $gh = a_1 x^{k_1} + a_2 x^{k_2} + \dots + a_{d-1} \cdot x^{k_{d-1}}$

ahol $0 \le k_1 < k_2 < \dots < k_{d-1} < n$
és $a_i \neq 0$ valamelyik i-re.

Ez jelentené azt, hogy gh polinomnak a Hamming súlya $\le d-1$.

gh polinomnak $\alpha, \alpha^2, \dots, \alpha^{d-1}$ gyökei, mert $g_1 | gh, \dots, g_{d-1} | gh$.

α gyök $\Leftrightarrow \alpha^{k_1} \cdot a_1 + \alpha^{k_2} a_2 + \dots + \alpha^{k_{d-1}} a_{d-1} = 0$

α^2 gyök $\Leftrightarrow (\alpha^{k_1})^2 \cdot a_1 + (\alpha^{k_2})^2 \cdot a_2 + \dots + (\alpha^{k_{d-1}})^2 \cdot a_{d-1} = 0$

$\vdots$

α^{d-1} gyök $\Leftrightarrow (\alpha^{k_1})^{d-1} \cdot a_1 + (\alpha^{k_2})^{d-1} \cdot a_2 + \dots + (\alpha^{k_{d-1}})^{d-1} \cdot a_{d-1} = 0$

$d-1$ egyenletből álló homogén lineáris egyenletrendszer, amelynek $(a_1, a_2, \dots, a_{d-1})$ nem triviális megoldása.

$$\det \begin{pmatrix} (\alpha^{k_1})^1 & \dots & (\alpha^{k_{d-1}})^1 \\ (\alpha^{k_1})^2 & & \vdots \\ \vdots & & \\ (\alpha^{k_1})^{d-1} & & (\alpha^{k_{d-1}})^{d-1} \end{pmatrix} = 0$$

$$\alpha^{k_1} \cdot \alpha^{k_2} \cdot \dots \cdot \alpha^{k_{d-1}} \cdot \det \begin{pmatrix} 1 & \dots & 1 \\ \alpha^{k_1} & & \alpha^{k_{d-1}} \\ \vdots & & \vdots \\ (\alpha^{k_1})^{d-2} & & (\alpha^{k_{d-1}})^{d-2} \end{pmatrix}$$

Vandermonde determináns.

$$0 = \alpha^{k_1} \cdots \alpha^{k_{d-1}} \cdot \prod_{i<j} \left(\alpha^{k_i} - \alpha^{k_j}\right)$$ ~~K-ban.~~ T-ben.

$$\Downarrow$$

$\exists\, i<j$ $\quad \alpha^{k_i} = \alpha^{k_j}$

$\alpha^{k_j - k_i} = 1 \qquad k_j - k_i < n$

de ez ellent mond annak, hogy α rendje legalább n.

Ezzel megmutattuk, hogy min távolság legalább d.